Synopsis

Submitted on

"A Secure and Verifiable Big Data Access Control System in Cloud"

For

Doctor of Philosophy in Computer Science and Engineering

To

SGGSIET, Nanded

Submitted By

EKDANTE SANTOSH GUNWANT (ME, MBA)

Department of Information of Technology

Shri Guru Gobind Singhji Institute of Engineering and Technology

ABSTRACT

1. Introduction:-

Big data is a high volume, high velocity and high variety of information in nature. Due to its complexity and large volume it outsource onto cloud server, that has the capabilities of storing data and processing users' access requests in an efficient manner. However when a data owner outsources its data to a cloud, sensitive information may be disclosed because the cloud server is not trusted; thereby typically the ciphertext of the data is stored in the cloud. But how to update the ciphertext stored in a cloud when new access policy is designed by the data owner and how to verify legitimacy of a user who intend to access the data are still of great concerns.

Most existing approaches for securing the outsourced big data in clouds are based on either attribute based encryption (ABE) or secret sharing to provide predefined the set of users for accessing the data but they suffer from high complexity of efficiently updating the access policy, ciphertext legitimacy user verification. It become more challenging and critical to deal with the issue of access policy update for enhancing security and dealing with dynamism caused by user join and leave activities.

On the other hand verifiable secret sharing based schemes rely on RSA (**Rivest, Shamir, Adleman**.-Popular RSA Algorithm) for multiple users need to be mutually verify their legitimacy. But RSA require high computation overhead and it could be broken by quantum computing in the near future. So to resist this quantum computing attack and making it urgent to exploit new techniques, based on cryptosystem is a type of lattice based cryptography NTRU (N-th degree Truncated polynomial Ring Units) is derived with lighting fast computational capability. However NTRU suffers from the problem of decryption failures. So to overcome the above mentioned problem and keep your data with secure, verifiable and authorization access control new NTRU cryptosystem is proposed to overcome

the decryption failure of the original NTRU. In the environment, cloud server can directly update the stored ciphertext without decryption of the data, based on the new access policy specified by the data owner who is able to validate the update at the cloud. The proposed scheme can verify the shared secret information to prevent users from cheating and can counter various attack such as the collusion attack.

2. Literature Review :-

Because big data frequently contain a huge amount of personal identifiable information, how to securely store the data and how to provide access control over the stored data are two biggest challenges. Outsourcing to clouds is one of the most popular approaches to securing big data storage in which the data owners encrypt their data based on cryptographic primitives and store the encrypted data to the clouds. Adequate access control is key to protect the stored data access control has traditionally been provided by operating systems or applications restricting access to the information, which typically exposes all the information if the system or application is hacked. A better approach is to protect the information using encryption that only allows decryption by authorized entities. Attribute based encryption (ABE) is one of the most powerful techniques for access control in the cloud systems. However it is difficult to update policies when ABE based schemes are applied because the data owners do not store the data in their local systems, once they outsource the data in to the cloud servers. It is also difficult to verify the legitimacy of the downloaded data as the clouds housing the data are not trustworthy. Beside the operation of the encryption and decryption in ABE have a high computational overhead and incure a large energy consumption.

Secret sharing is another powerful technique to protect the big data in cloud storage the most related work to our proposed scheme [14] and [15] whose verification procedure can resist potential attacks such as collusion and cheating. In [15] two schemes were proposed namely scheme-1 and scheme-2, based on the homogeneous linear recursion and the RAS cryptosystem, in which the homogeneous linear recursion is used to construct the secret share and reconstruct the secret, the RSA is used to verify the users' access legitimacy which leads to generate linear computational complexity, and the RSA cryptosystem which is used for

verification. In this schemes, as multiple users mutually verify each other using multiple RAS operations, a very high computational overhead occurs. In addition, classic asymmetric crypto solutions would be broken by quantum computing; that is this traditional verification methods can not satisfy the verification requirements with respect to quantum computing. Thus, we need to seek new verification methods to meet the future requirement. For this purpose utilize the NTRU cryptosystem to counter the quantum computing attacks. In case of delegation of private key / cipher-text was designed for third party to re-encrypt the ciphertext to a more restrictive policy using only public information these two approaches cannot satisfy our security requirements because they delegate the privet key / ciphertext for a new access policy that more restrictive than the earlier one – in perspective the access policy to a ciphertext might need to be relaxed as time goes for many real world applications. Therefore in [11], they allow the new access policy designed by the data owner to be independent than the previous one, and the ciphertxt is updated by the cloud based on new access policy [15].

3. Problem Statements:-

In the present era, companies, and organizations are facing the challenges to effectively manage their complex data. As the development of cloud storage, outsourcing the data to a cloud is an appropriate approach. For example, the IBM cloud was proposed as a public one for the data management of banking. When a bank stores its data in the cloud server only its legal staff members have the rights to access the stored data. Typically, the bank system contains much sensitive and private consumer information. In order to reduce the risk of information leakage, the access right of an employee should be restricted, and a single employee should not be allowed to reveal the data by itself without obtaining the authorization from other users; that is recovering the data requires to get the authorization of multiple employees. Moreover, the bank should be able to update the access policies for the stored data in a dynamic and efficient manner. Such applications usually require the data to be stored in a cloud in ciphertext format, and the access of the data by user requires multiple other users to verify the access legitimacy of the user.

4. Proposed System:-

To overcome the above given challenges, first, a plaintext data is bound to a secret that is shared by all legitimate users of the data based on (t, n)-threshold secret sharing, where 't' is the threshold value designated by owner that at least 't' legitimate user permission needs to manipulate the data and 'n' indicate data owner splits the access right of an encrypted plaintext into n pieces for n users, with one piece for each legitimate user of the data. A message certificate is computed for the data based on the NTRU encryption; the cipher-text is produced from both the shared secret and the message certificate. Second, the legitimacy of a user for accessing the data is verified by both the data owner and at least t-1 other legal users of the data, and the information provided by other users for the plaintext recovery needs to be validated by the users to prevent against cheating behaviors. Third, the plaintext data can be obtained when at least t-1 other users participate in the recovery process and provide correct information for the data recovery, based on (t, n)- threshold secret sharing. Last, the access policy of the data and the secret shares bound to the data can be dynamically changed by the data owner, and the update of the ciphertext is conducted by the cloud server without the need of downloading the previous ciphertext from the cloud to the data owner. Meanwhile, the data owner is able to verify whether the ciphertext stored in the cloud is correctly updated. We intend to achieve the following security objectives when designing our access control scheme for big data storage in clouds.

Data confidentiality: The outsourced data must be protected from eavesdropping attacks during upload, download, update, and retrieval of the data. Verification: The legitimacy of any user to access the data must be variable; the information provided by any user for plaintext recovery must be validated. Attack resistance: The proposed scheme must be able to counter potential attacks (cheating, collusion attack, forging attack, etc) launched by misbehaving users and adversaries.

But existing cryptographic primitives NTRU and Secret sharing proved to be faster than RSA, but both getting plaintext recovery is extremely high. From this NTRU we mostly face wrap failure & Gap failure and from secret sharing a user may cheat when recovering the secret S. For example, a user Ui may provide an incorrect Si, making recover S fail. In order to overcome this problem, verifiable secret sharing schemes have been proposed, which are mainly based on the RSA cryptosystem that incurs high computational

overhead. So we need to propose a new validation method to prevent a user from submitting fake information for the correct message recovery based on the NTRU cryptosystem. There exist two types of decryption failures in NTRU: the Wrap failure and the Gap failures. In other words, the decryption process on NTRU cannot always output a correct decryption message. To overcome this problem, we require new method to Improved NTRU cryptosystem to successfully get rid of the two types of decryption failures.

5. Future Research Plan:-

In our proposed system we are going to used four novel method to propose a secure and verifiable access control scheme for big data storage that tackle the following challenges

- How to securely store the data in a cloud server and distribute the shares of the access right to all legitimate users of the data?
- How to verify the legitimacy of user for accessing the data?
- How to recover the plaintext data when the access right needs to be jointly granted by multiple users
- How to dynamically and efficiently update the cipher-text in the cloud when the access policy of the data is changed by the data owner?

6. Conclusion:-

This Scheme allows the data owner to dynamically update the data access policy and the cloud server to successfully update the corresponding cipher-text to enable efficient access control to over the big data in cloud. It also provides a verification process for a user to validate its legitimacy of accessing both data owner and legitimate users.

References: -

[1] A. Sahai and B. Waters, “Fuzzy identity-based ecryption,’’ in advances in Cryptology, Berlin, Germany: Springer, 2005, pp457-473

[2] C.Hu, F. Zhang, X. Cheng, X Liao, and D.Chen, "Security communications between external users and wireless body area networks," in Proc. 2nd ACM workshop Hot Topic WirelessNetw. Secur. Privacy, 2013, pp.31-36

[3] C.Hu, X Cheng, Z Tian, J. Yu, K Akkaya, and L.Sun, " An attribute-based signcryption scheme to secure attribute-defined multicast communications" in Proc. 11th EAI Int. Conf. SecureComm, 2015, pp.418-435

[4] A Shamir, "Identity-based cryptosystem and signature schemes " in Advances in Cryptology. Berlin, Germany: 1985, pp 47-53

[5] M. Dehkordi and S. Mashhadi, "An efficient threshold verifiable mult-secret sharing," Comput. Standards Interfaces, Vol 30, no.3, pp 187-190,2008.

[6] O. Rgev, "New lattice based cryptographic construction," J ACM, vol51, no 6 pp.899-942, 2004

[7] V.C. Hu, D Ferraiolo, and D.R Kuhn, "Assessment of access control systems," US Dept. Commerce, Nat Inst. Standards technol., Gaithersburg, MD, USA Tech Rep. 7316, 2006

[8] The NTRU Public Key Cryptosystem- A tutorial, NTRU Cryptosystems, Wilmington, MA, USA, 1998

[9] K. Yang and X. Jia, "Attributed based access control for multi-authority systems in cloud storage," in Proc. IEEE 32nd Int. Conf. Distrib. Comput. Syst., 2012, pp. 536-545

[10] A. Sahai, H. Seyalioglu, and B. Waters, " Dynamic credentials and ciphertext delegation for attribute based encryption," in Advances in Cryptology. Berlin, Germany: Sprin.ger, 2012, pp. 199-217

[11] C.Hu, X. Liao, and D. Xiao, "Secrete image sharing based on chaotic map and Chinese remainder theorem," Int. J. Waveletes Multiresolution Inf. Process., Vol. 10, no.3, 2012, Art. No. 1250023

[12] IBM, "IBM storage solutions for banking," (2015). [Online]. Available: http://www-03.ibm.com/system/storage/solutions/industries/banking.html

[13] A. Corcoles, et al., "Demonstration of a quantum error detection code using a square lattice of four superconducting qubits," Nature Commun., vol. 6, pp. 1-10, 2015.

[14] Z. Eslami and J. Z. Ahmadabadi, "A verifiable multi-secret sharing scheme based on cellular automata," Inf. Sci., vol. 180, no. 15, pp. 2889- 2894, 2010

[15] M.H. Dehkordi and S. Mashhadi, “New efficient and practical verifiable multi-secret sharing scheme,” omput. Standards Interfaces, vol. 29, no. 1, pp. 138-141, 2007

Assist. Prof. S. G. Ekdante
Research Scholar

Dr. Arati K. Manjramkar
Research Guide